STEPHANIE M. HINDS (CABN 154284)
Acting United States Attorney

HALLIE HOFFMAN (CABN 210020)
Chief, Criminal Division

DAVID COUNTRYMAN (CABN 226995)
CHRIS KALTSAS (NYBN 5460902)
CLAUDIA A. QUIROZ (CABN 254419)
WILLIAM FRENTZEN (LABN 24421)
Assistant United States Attorneys

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-436-7428
FAX: (415) 436-7234
claudia.quiroz@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. Approximately 69,370 Bitcoin (BTC), Bitcoin Gold (BTG), Bitcoin SV (BSV), and Bitcoin Cash (BCH) seized from 1HQ3Go3ggs8pFnXuHVHRytPCq5fGG8Hbhx Defendant. ILIJA MATUSKO, Claimant.	CASE NO. CV 20-7811 RS **DECLARATION OF JEREMIAH HAYNIE IN SUPPORT OF UNITED STATES' MOTION TO STRIKE THE VERIFIED CLAIM OF CLAIMANT ILIJA MATUSKO** Hearing Date: September 30, 2021 Time: 1:30 p.m. Court: Hon. Richard Seeborg

I, JEREMIAH HAYNIE, state as follows:

1. I am a Special Agent with the Criminal Investigation Division of the Internal Revenue Service ("IRS-CI"). I am a case agent assigned to this case. I respectfully submit this declaration to

provide certain relevant information in support of the United States' Motion to Strike the Verified Claim of Ilija Matusko. I personally conducted the blockchain analysis of the bitcoin at issue in this case and was involved in the investigation from its inception to the present day.

A. Silk Road User Registration

2. Ross Ulbricht went to great lengths to ensure that buyers and sellers on Silk Road were able to operate anonymously. The subtitle of Silk Road was "anonymous market." *See* Exhibit 1 attached hereto. Consistent with the operation of an anonymous market, Silk Road users were required to provide very little identifying information. Users that registered with Silk Road were required to provide a username and a password. Users could optionally provide a country of residence, write a description, and upload an image. Of note, the user was not required and was not asked to provide identifying information such as a real name, physical address,[1] social security number, date of birth, email address, or phone number. In addition, a user was not required to deposit bitcoin or pay a fee to register an account on Silk Road. I know this because various law enforcement agents opened accounts with Silk Road as part of different investigations and did not have to deposit bitcoin or pay a fee.

3. The registration process for Silk Road differs greatly from the processes required from cryptocurrency exchanges such as Coinbase, Kraken, Binance, and others. Unlike Silk Road, reputable exchangers and cryptocurrency companies require users of their respective platforms to conform with relevant laws and regulations, including those set forth by the Bank Secrecy Act and related regulations, such as "Know Your Customer" (or "KYC") requirements. Prospective customers of those exchanges are thus required to confirm their identities prior to trading or purchasing cryptocurrencies on those exchanges, and anything used to obtain confirmation of that identity is obtainable by law enforcement. Conversely, Silk Road went to great lengths to maintain privacy and anonymity of its users, and so required no proof of identity. Indeed, doing so would have completely undermined the purpose of Silk Road.

[1] In some instances, buyers provided vendors with a physical mailing address in order to receive drug shipments. Due to the fact that users were receiving drugs, individuals in online forums often advised buyers to use addresses not associated with the buyer in case the packages were interdicted.

4. On approximately October 2, 2013, as part of their investigation into Silk Road and Ross Ulbricht, the FBI seized a server that contained information about Silk Road users. Within this data was a table[2] labeled "users" that contained registration information about Silk Road users. Exhibit 2, attached and shown below, is an export of the information that the table labeled "users" contained for hanson5.[3]

index	123591
id	cfaf83c718
user	hanson5
pass	[Redacted]
pin	
pin_attempts	0
bc_addr	
usalt	[Redacted]
available	47.52
tx_lock	0
credit_limit	0
average_rating	0
total_weight	0
rank	0
rating	0
buyer_weight	0
vendor_weight	0
transactions	0
description	This user has yet to enter a description
location	Germany
ship_from	
ship_to	
domestic_only	1
sort_by	
rating_sort	weight
role	0
active	0
peg	36
hedge	0
display_price	0
currency_id	37
incognito	0
commission_pricing	0
stealth_mode	0
auto_withdraw	0
auto_withdraw_address_1	
auto_withdraw_address_2	
auto_withdraw_address_3	
last_action	1352091317 [Converts from Unix Time to November 5, 2012 04:55:17 UTC]
last_bitcoin_request	1344382552 [Converts from Unix Time to August 7, 2012 23:35:52 UTC]
read_announcement	1
seller_start	0
seller_ban	0
discussion_ban	0
alias	hanson5
bond_refund	0
last_user_agent	
created	1325034975 [Converts from Unix Time to December 28, 2011 01:16:15 UTC]
modified	1325034975 [Converts from Unix Time to December 28, 2011 01:16:15 UTC]

[2] SQL databases are made up of tables that store data in rows and columns, similar to spreadsheets.

[3] The "pass" value appeared to be a hashed password, meaning that it was not stored in clear text. The "usalt" value suggested that the password was salted, meaning extra characters were added to it before it was hashed. I redacted the password and salt values to protect the claimant from password re-use attacks. I also converted the Unix time to a readable date/time format where noted.

B. Flow of Bitcoin Through Silk Road

5. Once a user deposited bitcoin to their assigned bitcoin address on Silk Road, their Silk Road account was credited with the requisite bitcoin, which Silk Road then used as it saw fit. For example, if User A deposited one bitcoin to the bitcoin address Silk Road assigned him, User A's account was credited with one bitcoin. The actual bitcoin contained within the Bitcoin address assigned to the user could then be used by Silk Road as needed. If, in the same example, User B requested a withdrawal of one bitcoin, Silk Road could have sent User B the one bitcoin it just received from User A. Even though the one bitcoin came from a Bitcoin address assigned to User A, User A's balance would not change.

6. This method of internal accounting is common outside the bitcoin world as well. For example, if a bank customer hands a $100 bill to a bank teller with instructions to deposit it to her account, the customer's account is credited with $100 and the actual $100 bill is put into the teller's till. The bank can do whatever it wants with the $100 bill and it will not affect the customer's account. For example, if a bank robber is next in line and demands the money from the teller, and the teller gives the bank robber the $100 bill, the customer's account is not reduced by $100.

7. When Individual X stole 70,411.46 bitcoin from Silk Road, the balance of the hanson5 account was not affected; it remained at 47.52 bitcoin. The bitcoin that Individual X stole originated from bitcoin addresses that were assigned to Silk Road users as deposit addresses, but just like the scenario in which $100 was stolen from the bank, the Silk Road user accounts had already received their credit, so the bitcoin stolen by Individual X was part of the Silk Road pool. Ulbricht did not deduct the user account balances by the amount that was stolen because the funds were not taken from specific user accounts. I am unaware of any public announcement of this theft by Ulbricht. This was also not a fatal event to the operation of Silk Road since Silk Road continued to operate for another 17 months before Ulbricht was arrested.

8. In summary, once a Silk Road user deposits bitcoin to their assigned address, their account is credited and the actual bitcoin that was deposited becomes part of the Silk Road pool.

C. Withdrawing Bitcoin from a Silk Road User Account

9. Matusko asserts that "[a]t no time did the Marketplace provide, nor did Mr. Matusko

know, the private key to access the Marketplace wallet or thereafter control the 48 bitcoin." The hanson5 accountholder did not require the Silk Road private key to withdraw bitcoin. Silk Road users could withdraw bitcoin from their account by simply accessing their account, entering the amount they wanted to withdraw, and the bitcoin address to send it to. All hanson5 had to do was log into the account and request a withdrawal.

10. Matusko wrote that, "Sometime later I realized that I had forgotten my password to my 'hanson5' user account and that I no longer had access to my account." Due to the anonymity Silk Road provided to its users, Silk Road did not have an official password recovery option for its users. However, a Google search of "Silk Road password reset" led to the following internet post dated June 7, 2013:

> *"If you forgot your password, unfortunately you will not be able to retrieve it. Some people have had success by creating a new account and messaging mods either on the forum or via the Road. If you can prove that you are the owner of the other account (By stating order history, bitcoin balance, pin code, etc.) then you* ***might*** *have some luck getting the account back."* [4]

D. *United States v. Twenty-Four Cryptocurrency Accounts* (Welcome to Video)

11. Matusko asserts that, "in similar bitcoin forfeiture actions, the government traced all transactions on the bitcoin blockchain and provided direct notice via certified mail and email to all potential users." He cites to *United States v. Twenty-Four Cryptocurrency Accounts*, 473 F. Supp. 3d 1 (D.D.C. 2020). The investigation that gave rise to *United States v. Twenty-Four Cryptocurrency Accounts* was an investigation of "Welcome To Video," a Tor-based website engaged in the sale of child sexual abuse material. I am familiar with this investigation and provided a small amount of assistance to the Special Agent charged with investigating the case.[5]

12. A major goal of the Welcome To Video investigation was to identify the purchasers of child sexual abuse material. The team recognized that a portion of bitcoin that was used to purchase child sexual abuse material originated from three specific exchanges known to require KYC information from their customers. The team used the identifying information collected by the exchanges as a

[4] https://www.reddit.com/r/SilkRoad/comments/1fve2n/password_reset/

[5] In October 2017, I, along with others in my group, were asked to conduct open-source searches to identify social media profiles of individuals who had purchased child sexual abuse material from Welcome To Video.

beginning step to identify the individuals that sent bitcoin to Welcome To Video. The team conducted additional investigative actions such as open-source searches, bitcoin tracing, interviews, surveillance, and physical search warrants to gather evidence about each accountholder. Numerous purchasers of child pornography on the site were prosecuted as a result of the investigation. On October 16, 2019, the United States filed a verified complaint for forfeiture *in rem* to seize the funds that remained in the exchange accounts held by the Welcome To Video customers.

13. In contrast, the investigation of the stolen Silk Road bitcoin did not require the identification of Silk Road users to determine the identity of the person responsible for stealing bitcoin from Silk Road. Moreover, Silk Road itself did not require its users to provide any KYC information, rendering information on Silk Road users unobtainable. Indeed, bitcoin sent to Silk Road did not need to flow through a hosted exchange; the bitcoin used to fuel accounts at Silk Road could have stemmed from either exchanges or unhosted wallets, which are far more difficult to trace than hosted wallets.

14. Finally, the technology to trace the deposits of cryptocurrency utilized in the Welcome to Video case was not widely available at the time of the Southern District of New York's seizure in 2013. Most commercial cryptocurrency tracing services in existence today did not exist, or were not fully established, at the time of the initial seizure.

15. Elliptic was founded in October 2013 (*see www.elliptic.co/our-story*). Chainalysis was founded in 2014 (*see https://web.archive.org/web/20170601100217/https://www.chainalysis.com/*). CipherTrace was founded in 2015 (*see https://ciphertrace.com/about-us/*).

E. Price of Bitcoin

16. The U.S. government seized the Silk Road servers and arrested Ross Ulbricht on or about October 2, 2013. The closing price of bitcoin on that date was approximately $140.30.[6] Accordingly, on October 2, 2013, the 47.52 bitcoin contained in the hanson5 account was valued at approximately $6,667.06.

F. Illegal Drugs Made Up More than 95 Percent of the Listings on Silk Road

17. According to exhibits (940 and 940A) presented during the Ulbricht trial, more than 95

[6] https://www.investing.com/crypto/bitcoin/historical-data

percent of all listings on the Silk Road Marketplace were illegal narcotics. The "Other" category included some illegal items, such as fake passports, and some legal items such as books.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed this 9th day of September, 2021 in East Lansing, Michigan.

/s/ Jeremiah Haynie
JEREMIAH HAYNIE
Special Agent
Internal Revenue Service – Criminal Investigation

Exhibit 1

Silk Road
anonymous market

messages 0 | orders 0 | account ฿0.0000 *$0.00*

Search [ ] Go

a few words from the Dread Pirate Roberts

Hi, **cirrus** *logout* 0

Shop by **Category**

- Drugs *13,810*
  - Cannabis *2,934*
  - Dissociatives *199*
  - Ecstasy *1,274*
  - Intoxicants *75*
  - Opioids *367*
  - Other *82*
  - Precursors *62*
  - Prescription *4,659*
  - Psychedelics *1,754*
  - Stimulants *1,634*
  - Tobacco *219*
- Apparel *767*
- Art *15*
- Books *1,322*
- Collectibles *27*
- Computer equipment *101*
- Custom Orders *86*
- Digital goods *886*
- Drug paraphernalia *512*
- Electronics *234*
- Erotica *584*
- Fireworks *35*
- Food *10*
- Forgeries *152*
- Hardware *35*
- Home & Garden *27*
- Jewelry *104*
- Lab Supplies *29*
- Lotteries & games *165*
- Medical *60*
- Money *258*
- Musical instruments *6*
- Packaging *95*
- Services *168*
- Sporting goods *4*
- Tickets *4*
- Writing *8*

Boldabol 200 (B. Dragon), 10ml, 200mg.ml
$66.11

PIRACETAM tbl. 100x1200mg (nootropil
$92.64

25X LSD BLOTTER
$421.19

7 grams of PURE MDMA Moonrocks.
$378.58

100x Green Android™ (The New Mortal Kombat™)
$547.65

2mg Xanax Bars from Wallgreens
$5.42

10.0g MDA - Reagent Tested
$550.00

HYDRO BUDS 2G
$40.00

SCIROXX - Nandrodex 300mg/ml 10ml USA ONLY
$114.21

10g Amnesia Haze
$194.77

4 Orange sunshine 300ug
$90.49

1/4 Bubba Kush
$90.20

From the forum
- Buyer ratings discussion
- Feedback system changes
- HOW TO: Run your own relay and help the Tor network!
- Ask a drug expert physician about drugs and health
- Winning the war on drugs
- New display currencies
- Try Tails for a more secure OS

Favorite vendors
- Dread Pirate Roberts 5.0 *remove*
- Libertas 1.0 - *remove*
- inigo 0.0 - *remove*

GOVERNMENT EXHIBIT 132
14 Cr. 68 (KBF)

฿1 = $133.74

community forums | wiki | support

SA-9

Exhibit 2

index	123591
id	cfaf83c718
user	hanson5
pass	[Redacted]
pin	
pin_attempts	0
bc_addr	
usalt	[Redacted]
available	47.52
tx_lock	0
credit_limit	0
average_rating	0
total_weight	0
rank	0
rating	0
buyer_weight	0
vendor_weight	0
transactions	0
description	This user has yet to enter a description
location	Germany
ship_from	
ship_to	
domestic_only	1
sort_by	
rating_sort	weight
role	0
active	0
peg	36
hedge	0
display_price	0
currency_id	37
incognito	0
commission_pricing	0
stealth_mode	0
auto_withdraw	0
auto_withdraw_address_1	
auto_withdraw_address_2	
auto_withdraw_address_3	
last_action	1352091317 [Converts from Unix Time to November 5, 2012 04:55:17 UTC]
last_bitcoin_request	1344382552 [Converts from Unix Time to August 7, 2012 23:35:52 UTC]
read_announcement	1
seller_start	0
seller_ban	0
discussion_ban	0
alias	hanson5
bond_refund	0
last_user_agent	
created	1325034975 [Converts from Unix Time to December 28, 2011 01:16:15 UTC]
modified	1325034975 [Converts from Unix Time to December 28, 2011 01:16:15 UTC]